IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

AUTHENTICOM, INC., Plaintiffs, v. CDK GLOBAL, LLC, and THE REYNOLDS AND REYNOLDS COMPANY, Defendants.	No. 3:17-CV-318-JDP

DEFENDANT THE REYNOLDS AND REYNOLDS COMPANY'S REPLY IN SUPPORT OF MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Peeling back the din and emotion of Authenticom's response in opposition ("Opposition," Dkt. 216) to Defendants' motions to dismiss reveals that Authenticom's claims are irreparably flawed. *First,* Authenticom's allegedly "restrained trade" is illegal. And *second,* it has no answer to *Trinko*: Reynolds is not required to help Authenticom peddle its illegal trade. Neither issue was addressed in this Court's orders regarding the injunction. And both are dispositive as a matter of law.

Authenticom's chosen business model—its allegedly "restrained trade," for antitrust purposes—is contingent upon gaining access to and exploiting Defendants' proprietary systems and software. Authenticom does not dispute this core characterization—indeed, it cannot, given the nature of its requested relief. But nothing in the antitrust laws allows one business to trespass upon the property of another. And certainly nothing compels a business to allow such trespass to occur free of charge or conditions. Indeed, as set forth in Reynolds's Memorandum in Support of Motion to Dismiss ("Memorandum," Dkt. 176), such actions are illegal and Authenticom's claims are contrary to established antitrust law. By contrast, the Reynolds technological measures and contractual restrictions that comprise Reynolds's "blocking" strategy have been in place for years, are unilateral, and are lawful.

The following summarizes the reasons the Court should dismiss Authenticom's complaint.

1. The "trade" that Authenticom claims is restrained is *illegal*. As a matter of law, Authenticom cannot bring a viable antitrust claim against Reynolds regarding any restraint of that unlawful trade.

2. Authenticom's allegations based on unilateral conduct have no conceivable basis in law and should not proceed beyond this motion to dismiss. There is no question that Reynolds

has the right to unilaterally block Authenticom from its system. *Trinko* is controlling on this point. It is undisputed that Reynolds made the unilateral decision to strictly control access to its system many years ago and that Reynolds does not have monopoly power. Authenticom's claims based on Reynolds's unilateral decision to block Authenticom must be dismissed (e.g., fourth cause of action for "monopolization" and fifth cause of action for "tortious interference").

3. For these same reasons, tying claims (third cause of action) and exclusive dealing claims (second cause of action) likewise fail. The complained-of agreements are additional means of Reynolds's unilateral protections of its system from unauthorized access. Reynolds has no obligation to open or share its system under *Trinko*.

4. Finally, Authenticom's horizontal conspiracy allegations (first cause of action) are implausible and based not on any actual agreement, but centrally on decisions and alleged price "effects" that occurred ***before*** the alleged conspiracy. The "conspiracy" allegations are plausibly explained by *unilateral*, not joint, conduct. It is implausible that Reynolds made any agreement with CDK regarding what *CDK* would do with its system access policies. And Authenticom now runs from its complaint's reliance on the February 2015 contracts to make this "conspiracy" claim. Instead Authenticom relies heavily on price increases in, at best, single-brand aftermarkets to demonstrate "effects." *See* Compl., Dkt. 1 at ¶ 176 and Opposition, Dkt. 216 at 3. Though attempting to artfully ignore the point now, Authenticom's only citation to any alleged "sharp" price increases by Reynolds occurred ***before*** the alleged conspiracy's start date. *Compare* Opp. at 16 (complaining of allegedly sharp price increases but not noting the *date* of those increases) *with* the cited testimony at Dkt. 165 at 54:3-9 (making clear that those alleged increases were *in* ***2013*** and earlier, years before any alleged conspiracy). To be sure, Reynolds's technology and contracts "block" Authenticom (and malicious hackers alike)—but they do so

based on decisions made unilaterally years before any alleged conspiracy. Authenticom's claims based on an implausible conspiracy must be dismissed.

For these reasons and those set forth in Reynolds's Memorandum, the complaint should be dismissed.

I. AUTHENTICOM'S ATTEMPT TO ROPE IN THE ENTIRE INJUNCTION HEARING RECORD IS INAPPROPRIATE, BUT STILL DOES NOT SAVE ITS CLAIMS

Authenticom refused to amend its complaint following the injunction hearing, but now implicitly admits its complaint is not sufficient under *Twombly*.[1] Authenticom's reliance on the preliminary injunction record to modify its claims, however, does not save them.

While the Seventh Circuit has held that a plaintiff may expand upon a complaint's allegations through briefing, *see Phillips v. Prudential Ins. Co. of Am.*, 714 F.3d 1017, 1020 (7th Cir. 2013), there is a marked difference between elaborating on an existing allegation and adding a new allegation altogether. *See, e.g.*, *Epstein v. Epstein*, 843 F.3d 1147, 1151 n.5 (7th Cir. 2016) (refusing to consider new allegation on appeal). Authenticom repeatedly crosses into the latter category. Indeed, it is readily apparent that Authenticom no longer stands by key portions of its complaint—including many of its characterizations of the Defendants' written 2015 agreements. But for all the reasons set forth below and in the original Memorandum, even the most aggressive and favorable cherry-picking of facts do not transform the deficient complaint into one with plausible antitrust claims.

[1] It is notable that Authenticom does not cite or evaluate *Twombly* (other than a passing reference in its introduction) in this proceeding on a motion to dismiss an antitrust complaint. Authenticom, in its unconstrained references to materials outside of the pleadings, impliedly admits that its *complaint* (the document at issue here, and on which substantial resources have already been spent) is insufficient.

II. AUTHENTICOM'S CFAA ARGUMENTS ARE UNAVAILING; AUTHENTICOM'S ILLEGAL TRADE IS FATAL TO ALL CLAIMS

As set forth in Reynolds's Memorandum, the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030, bars all of Authenticom's claims as a matter of law. Under the statute's plain text, Authenticom's purportedly restrained trade—which consists of accessing Reynolds's systems without Reynolds's authorization to scrape information—is illegal. It is not coincidence that Authenticom's response to the illegality of its requested relief is buried on page 47 of its Opposition. Authenticom attempts to sidestep this illegality in three ways. All are unsuccessful.

A. This is not *in pari delicto*—the illegality of Authenticom's purported "trade" deprives Authenticom of any valid antitrust injury

First, Authenticom mischaracterizes Reynolds's argument as an *in pari delicto* defense. That is inaccurate: *in pari delicto* arises when the plaintiff "is himself involved in some of the same sort of wrongdoing" as the defendant. *Perma Life Mufflers, Inc. v. Int'l Parts Corp.*, 392 U.S. 134 (1968); *see also Gen. Leaseways, Inc. v. Nat'l Truck Leasing Ass'n*, 830 F.2d 716, 720-21, 724 (7th Cir. 1987) (permitting this defense only where the plaintiff "bore substantially equal responsibility for the anticompetitive restrictions"). The cases cited by Authenticom have held that this common law defense should not be broadly applied where doing so would undermine the objectives of antitrust law.[2]

[2] *Consol. Express, Inc. v. New York Shipping Ass'n*, 602 F.2d 494 (3d Cir. 1979), held only that that an antitrust plaintiff's "improper conduct did not preclude that plaintiff from asserting an antitrust claim unrelated to the improper conduct." *In re Wellbutrin XI Antitrust Litig. Indirect Purchaser Class*, --- F.3d. ----, No. 15-2875, 2017 WL 3531069, at *19 (3d Cir. Aug. 9, 2017). The same is true of *Pinto Trucking Service, Inc. v. Motor Dispatch, Inc.*, 649 F.2d 530 (7th Cir. 1981); *see Gen. Leaseways*, 830 F.2d at 722. Authenticom relies on *Memorex Corp. v. Int'l Bus. Machs. Corp.*, 555 F.2d 1379 (9th Cir. 1977), but "[t]he *Memorex* Court specifically left open the question of whether a violation of the law could bar an anti-trust action." *Pearl Music Co. v. Recording Indus. Ass'n of Am., Inc.*, 460 F. Supp. 1060, 1068 (C.D. Cal. 1978); *see also RealNetworks, Inc. v. DVD Copy Control Ass'n*, Nos. 08-4548, 2010 WL 145098, at *6 (N.D. Cal. Jan. 8, 2010) (distinguishing *Memorex* and finding that no antitrust injury could arise from

But the scenario here is of a very different species: Authenticom is seeking to enlist the antitrust laws to aid and protect a business practice that directly violates a different federal criminal statute (and numerous state laws). Courts have uniformly held that the antitrust laws do not protect such "trades" from restraint—both before and after *Perma Life*. *See, e.g.*, *Maltz v. Sax*, 134 F.2d 2, 4-5 (7th Cir. 1943); *Bubis v. Blanton*, 885 F.2d 317, 319-20 (6th Cir. 1989); *Pearl Music Co. v. Recording Indus. Ass'n of Am., Inc.*, 460 F. Supp. 1060, 1068 (C.D. Cal. Nov. 15, 1978); *RealNetworks, Inc. v. DVD Copy Control Ass'n*, Nos. 08-4548, 2010 WL 145098, at *6 (N.D. Cal. Jan. 8, 2010). Authenticom cites no case holding that the Sherman Act nonetheless protects an illegal trade.

Indeed, under Authenticom's reading of *Perma Life*, purveyors of pirated music, child pornography, or counterfeit or stolen goods could bring an antitrust action alleging an actionable refusal to deal or other supposed restraints on their "business." The Seventh Circuit squarely rejected this untenable outcome in *Maltz*: "[Since] the Anti-Trust Act … was a public benefit measure, it … seems rather paradoxical to permit plaintiff to invoke its protection for a business, the practice of which is against public policy, if not illegal." 134 F.2d at 4. Antitrust law does not permit relief "for an injury to something which the law did not recognize as a legal right." *Id.* at 5; *see also, e.g.*, *Pearl Music*, 460 F. Supp. at 1067-68 (illegal sales of pirated music not protected by antitrust laws). Nothing in *Perma Life* (or Authenticom's other cited cases) casts any doubt on that core logic—to the contrary, the allegedly restrained trade in *Perma Life* was the sale of automobile exhaust parts, which is legal. *See* 392 U.S. at 137.[3]

---

the defendant's refusal to license technology for a product that "is almost certainly illegal" under the Digital Millennium Copyright Act).

[3] *Maltz*'s holding on this point was independent of its "unclean hands" rationale. *See* 134 F.2d at 5. Whether or not the latter survives *Perma Life* and the Supreme Court's rejection of an

Authenticom's assertion (at 51) that its business is not "*independently* unlawful" further fails to distinguish this precedent. Reynolds and CDK are only accused of restraining the part of Authenticom's business (hostile unauthorized access to the DMS) that *is unlawful* under the CFAA (and similar state statutes). And it does not matter that the crime in question turns on whether the system owner authorized the putative rival's access. A music pirate's actions are only illegal because the record labels refuse to freely license their works, yet no antitrust liability lies there. *See Pearl Music*, 460 F. Supp. at 1067-68. Indeed, property crimes commonly turn on whether the owner has authorized the access to, or appropriation or use of, its property; that is the essence of ownership. This is true of both federal crimes, *see, e.g.*, 17 U.S.C. §§ 106, 506(a) (copyright infringement); 18 U.S.C. § 1832(a) (trade secret theft); § 2701(a) (unlawful access to stored communications), and state crimes, *see, e.g.*, Wis. Stat. § 943.13 (trespass); § 943.201 (misappropriation of personal identifying information); § 943.207 (transfer of recorded sounds); § 943.23 (operating a vehicle without owner's consent); § 943.49 (unlawful use of recording device). Nothing in the antitrust laws overrides laws criminalizing misuse of another's property without consent. Authenticom is not entitled to trespass upon the property of Reynolds or CDK to ply its trade, let alone free of charge.

Authenticom repeatedly asserts that a criminal statute cannot serve as an "antitrust immunity statute," positing that "if CDK and Reynolds violated Section 1 by agreeing to block Authenticom's access … the CFAA does not affect Authenticom's antitrust challenge." Opp. at 3. Authenticom has it backwards. Reynolds is not suggesting the CFAA immunizes antitrust

---

antitrust unclean hands defense in *Kiefer-Stewart Co. v. Joseph E. Seagram & Sons*, 340 U.S. 211, 214 (1951), those cases do not affect the continuing validity of *Maltz*'s separate holding.

violations; instead, there is no antitrust violation in the first place because the antitrust laws do not protect illegal trade from injury.

B. *hiQ* does not help Authenticom

Continuing its staunch refusal to answer *Trinko*'s caution against forcing firms to cooperate with putative rivals, Authenticom next contends (at 55-56) that there is no CFAA violation if Reynolds withheld authorization for illicit reasons, invoking *hiQ Labs, Inc. v. LinkedIn Corp.*, --- F. Supp. 3d ----, No. 17-cv-03301, 2017 WL 3473663 (N.D. Cal. Aug. 14, 2017), *appeal filed* No. 17-16783 (9th Cir. 2017). But *hiQ* does not help Authenticom.

First, the decision whether to grant Authenticom (and other third parties) authorization to access the DMS is a unilateral act not subject to Section 1. As discussed below, the only limits on Reynolds's right to deny access to its systems are set by *Trinko* and *Aspen Skiing*, and Authenticom does not even contend that those limits are implicated here. The law is clear that Reynolds had "no obligation to be kindly or cooperative toward other producers." *Sanderson v. Culligan Int'l Co.*, 415 F.3d 620, 623 (7th Cir. 2005).

Second, Authenticom's citation to *hiQ* is inapt—the *hiQ* trial court found no "unauthorized access" under the CFAA only because the defendant was "access[ing] LinkedIn *public* profiles." 2017 WL 3473663, at *4 (emphasis added). The court contrasted this with *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), *petition for cert. filed*, (U.S. Mar. 9, 2017) (No. 16-1105), where "[t]he defendant gained access to password-protected Facebook members profiles when its users supplied their Facebook login credentials" but Facebook itself refused to authorize such access. 2017 WL 3473663, at *4. As *hiQ* emphasized, "none of the data in *Facebook* … was *public* data." *Id.* at *5.

Rather, in *Facebook*, "the unauthorized intruders reached into what would fairly be characterized as the private interior of a computer system not visible to the public." *Id.* This is

the very conduct the CFAA outlaws—"'hacking' or 'trespass' onto private, often password-protected mainframe computers," *id.* (citing congressional reports)—and the very transgression Authenticom commits. Reynolds's system is *not* a public website, nor does Authenticom seek to retrieve publicly accessible information; the DMS is a password-protected, private, proprietary, networked enterprise computer system that Reynolds restricts for operability, performance, and security. The *hiQ* decision undercuts, rather than supports, Authenticom's argument.

Authenticom's reliance (at 56-57) on *Assessment Techs. of Wisconsin, LLC v. WIREdata Inc.*, 350 F.3d 640 (7th Cir. 2003), is equally inapt. As set forth in the Memorandum, that case, which did not involve the CFAA, merely held that the Copyright Act did not empower a putative copyright owner to forbid any disclosure of compiled public data that were neither copyrighted, nor created or obtained by the owner. *Id.* at 641-42. The Seventh Circuit did, however, point to contract and tort law as ways to prevent unauthorized access to databases and to enable owners "to recoup the expense of creating the database." *Id.* at 645-46. That is exactly what Reynolds does.

C. Authenticom's efforts to distinguish *Facebook* fail, as does its attempt to construe "authorization" as depending on dealers' rather than Reynolds's permission

Authenticom's third argument is that its conduct does not actually violate the CFAA, contending that dealers' granting of permission to Authenticom is sufficient "authorization" under the statute. But this argument is inconsistent with the statute's plain text, which properly turns on the authorization of the owner or administrator of a computer system, not merely the owners of information stored therein.[4] Additionally, Authenticom's efforts to construe

[4] *See* CA7 Oral Arg. at 50:00-50 ("But it [the dealer's consent] is not being granted by the person who runs the system. That is, by CDK or Reynolds. This [statute] doesn't say permission by anyone. If I have an account with AOL, to take a computer giant of the past, to get access to

Facebook as supporting its interpretation fail egregiously; instead, the Ninth Circuit plainly and properly rejected Authenticom's position.

As discussed in the Memorandum, the CFAA prohibits various actions related to a "protected computer" that are undertaken either "without authorization" or that "exceed authorization." 18 U.S.C. § 1030. Authenticom contends that authorization in question may be supplied solely by an owner of information stored within a protected computer. Even taking as true the allegation that Authenticom's requested system access is limited to data belonging exclusively to the dealer (which we know from the preliminary injunction record is not true, as it is also owned by automotive manufactures, Reynolds, and other third parties), Authenticom misreads the statute. Dealers cannot unilaterally sublicense, sell, or otherwise provide third party access to Reynolds's system as a matter of federal law.

Authenticom's statutory argument is based on *one* subparagraph of the CFAA, which provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer" commits an offense. 18 U.S.C. § 1030(a)(2)(C). Even considering this subparagraph in isolation, Authenticom's construction cannot be reconciled with the statutory text. This subparagraph criminalizes obtaining *any* information by unauthorized access of a computer, without limitation based on ownership. Nor would such a limitation make sense. Congress certainly did not intend to permit hacking into another's computer simply because one may own information stored therein. *See* CA7 Oral Arg. at 53:30-40 ("The word 'authorization' has to mean the same thing for the data in an NSA computer as it does for data in a Reynolds computer.") (Easterbrook, J.).

AOL's system you need AOL's permission, not my permission. The fact that I have an account with AOL doesn't mean I can authorize anyone else to use AOL.") (Easterbrook, J.).

Regardless, subparagraph (a)(2)(C) must be interpreted in context. The required element of "access[ing] a computer without authorization" applies to eight different enumerated CFAA offenses, many of which do not require that any particular information be obtained. *See id.* § 1030(a)(1), (2)(A)-(B), (3)-(7). Those that do cannot be construed to require only the authorization of the information owner. *See, e.g., id.* § 1030(a)(1) (prohibition of accessing a computer without authorization to obtain information restricted on national security grounds). Presumptively, "'identical words used in different parts of the same act are intended to have the same meaning.'" *Comm'r v. Keystone Consol. Indus., Inc.*, 508 U.S. 152, 159 (1993) (citation omitted); *see also United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (applying presumption to the CFAA). The CFAA criminalizes access unauthorized by the entity that owns or controls the computer, not merely by the owner of some portion of the information residing therein. See *United States v. Nosal*, 844 F.3d 1024, 1035-36 (9th Cir. 2016) (company that "owned and controlled access to its computers … retained exclusive discretion to issue or revoke access to the database").

As the Ninth Circuit held in *Facebook*, "[p]ermission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter," notifying the defendant "that it was no longer authorized to access Facebook's computers." 844 F.3d at 1067-68 & n.3. Drawing an analogy to a bank safe deposit box, the court explained that

> to access the safe deposit box, the person needs permission *both* from his friend (who controls access to the safe) *and* from the bank (which controls access to its premises). Similarly, for Power to continue its campaign using Facebook's computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers).

Id. at 1068. Authenticom's dealer authorization is no defense under the CFAA, especially after being notified that Reynolds objected.

Authenticom tries to distinguish *Facebook* by claiming that the defendant there "sought to access … '*Facebook's* data'—not just the user's data." Opp. at 53 (citations omitted). But this distinction fails: the Ninth Circuit's bank analogy expressly assumed that Power was seeking to access users' data stored on Facebook's servers. Authenticom's other distinction that Facebook "control[ed] the creation of usernames and passwords" whereas "Reynolds authorizes dealers to create their own usernames and passwords to access the DMS," Authenticom Br. 60, is also irrelevant and wrong. The username and password given to Power was created by the Facebook user. *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1028 (N.D. Cal. 2012).[5]

In sum, Authenticom's past, present, and future efforts to access Reynolds's DMS without Reynolds's authorization constitute clear violations of the CFAA. Authenticom's own pleaded facts establish these violations as a matter of law, which is fatal to all of its claims.

D. Authenticom has no answer to its other statutory violations

In addition to offering an unavailing construction of the CFAA, Authenticom also fails to address the other legal sources that similarly outlaw its chosen business of hostile integration. Authenticom altogether ignores California's computer crime statute, which, as quoted in the Memorandum (at 14), outlaws any action that "knowingly and without permission uses or causes to be used computer services." Cal. Penal Code § 502(c). The California statute uses the phrase "without permission" instead of "without authorization," but for these purposes the analysis is the same as under the CFAA. Indeed, as also cited in the Memorandum, case law interpreting the "without permission" element makes clear that the permission in question must come from

[5] Other courts have similarly held that user-granted "authorization" alone (where the user lacked authority to grant authorization) does not suffice under statutes protecting access to computer data. *See, e.g.*, *Nosal*, 844 F.3d at 1035-36; *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009); Memorandum at 16-20 (citing cases). Authenticom has no response to this uniform line of authority.

the computer system's owner or administrator, not a mere user. *See, e.g., Oracle USA, Inc. v. Rimini St., Inc.*, 191 F. Supp. 3d 1134, 1143 (D. Nev. 2016); *Satmodo, LLC v. Whenever Commc'ns, LLC*, 17-CV-0192-AJB NLS, 2017 WL 1365839, at *6 (S.D. Cal. Apr. 14, 2017). Any action taken without that owner's consent, or in violation of its specified terms of use, is outlawed.

Authenticom also waves aside Reynolds's arguments regarding the WCCA in a footnote (Opp. at 52 n.8), contending that Authenticom has not improperly disclosed any access codes. That misses the point: the statute prohibits ""[d]isclos[ing] restricted access codes . . . to unauthorized persons," and Authenticom itself, along with its employees, are unauthorized persons. Wis. Stat. § 943.70(2)(a)(6). Authenticom admits it passes [wrongfully obtained] access codes to its employees. Authenticom also ignores the other provision cited in Reynolds's Memorandum, which makes clear that in Wisconsin it is illegal to "[a]ccess[] computer programs" without authorization, regardless of whether information is obtained. *Id.* § 943.70(2)(a)(3). Each time Authenticom accesses the Reynolds programs that comprise the DMS, Authenticom violates the WCCA. Authenticom offers no argument in response.

III. AUTHENTICOM HAS NO ANSWER TO *TRINKO*, AND REYNOLDS FUNDAMENTALLY HAS NO DUTY TO ALLOW AUTHENTICOM'S DESIRED DMS ACCESS

As set forth in the Memorandum, the Supreme Court's decision in *Trinko* makes clear that Reynolds has no duty to deal with or assist Authenticom (or any other purported integrator). Memo. at 27, 30-33; *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004). As made clear in this proceeding and in its Seventh Circuit argument, Authenticom has no answer to *Trinko*. *See* CA7 Oral Arg. at 30:10-20 ("Both Judge Wood and I have been asking questions about *Trinko* and *Linkline*, and you have not really engaged.") (Easterbrook, J.). Businesses are generally "free to choose the parties with whom they will deal,

as well as the prices, terms, and conditions of that dealing," *Pac. Bell Tel. Co. v. Linkline Commc'ns, Inc.*, 555 U.S. 438, 448 (2009), and Reynolds has never had any obligation to grant Authenticom the access it demands.

Authenticom's sole response is to contend that "[n]othing in Authenticom's complaint seeks Defendants' *cooperation* or requires a regime of 'forced sharing.'" Opp. at 47 (quoting *Trinko*, 540 U.S. at 408). That contention is spurious. *First*, this entire case is about Authenticom's desire to use and access Defendants' proprietary DMS systems and software through automated queries and Reynolds's desire to prevent it. Authenticom affirmatively pleads that it cannot ply its chosen "trade" without using Defendants' servers and software, and its entire alleged injury flows from the deprivation of that use. Authenticom attempts to obfuscate this by talking primarily about its need for "data," but the complaint makes clear that Authenticom's claims all hinge upon the denial of system access, not mere data access. *See, e.g.*, Compl. ¶¶ 49-50, 53, 56, 77 (all making clear that Authenticom's "integration" service is dependent on having and exploiting direct access to the DMS).

Second, this Court has already recognized the certainty that the injunction requested by Authenticom specifically requires Reynolds's forced cooperation. *See* Order, Dkt. 172 at 21 ("[T]he court did receive evidence that a preliminary injunction may require defendants to **adjust their systems** to accommodate Authenticom's access, and that **such efforts may be costly**.") (emphasis added); *see also* Order, Dkt. 192, at 3 ("**Reynolds must configure** Authenticom's login credentials within five business days of receiving a dealer authorization form from Authenticom.") (emphasis added); *id.* ("The dealer authorization form will also provide that the dealer authorizes **Reynolds to suspend security measures** directed specifically to blocking automated access for the Authenticom-specific credentials.") (emphasis added).

Authenticom's requested relief—for Defendants to "stop blocking" Authenticom's access to their proprietary DMSs—is forced sharing at its most extreme. Authenticom's demand runs headlong into the principle that the antitrust laws are not intended to undermine businesses' "confidence that they can control access to their own property, real or intellectual." *Four Corners Nephrology Associates, P.C. v. Mercy Med. Ctr. of Durango*, 582 F.3d 1216, 1221 (10th Cir. 2009). Thus, the mere fact that Authenticom wants the forced sharing to be for free, unrestrained by any actual licensing terms and conditions, does not remove this case from *Trinko*'s scope. To the contrary, Authenticom's demand for such patently unfair terms simply highlights the legitimacy of Defendants' refusals to provide Authenticom with its desired access. The antitrust laws generally impose no duty "to cooperate with rivals by selling them products that would help the rivals to compete," *Schor v. Abbott Labs.*, 457 F.3d 608, 610 (7th Cir. 2006) (citing *Trinko*, 540 U.S. at 408); they surely do not entitle a rival to exploit another business's property without authorization or compensation.

Authenticom's professed need to service its "voluntary business relationships" free from interference does not change the analysis either. *Cf.* Opp. at 47. Whatever their terms, Authenticom's other relationships cannot alter Reynolds's and CDK's fundamental rights not to license their DMS technologies to Authenticom—and especially to not do so for free and free of licensing restrictions. Authenticom cannot create a right of DMS access simply by demanding or promising such access in a third party contract, nor can it contend that Reynolds's refusal to acquiesce to such arrangements constitutes "interference." Reynolds has the right to block Authenticom—and DMI, IntegraLink, and SelectQu—and further to grant or deny access to its proprietary system on any terms it deems appropriate. *See, e.g., CBC Companies, Inc. v. Equifax, Inc.*, 561 F.3d 569 (6th Cir. 2009) (rejecting challenge to credit bureau's unilaterally

imposed contractual restriction). Just as the owner of a ski resort may decide to "reserve to itself the right to provide ancillary services," so too may the operator and licensor of an enterprise computer system. *See Christy Sports, LLC v. Deer Valley Resort Co., Ltd.*, 555 F.3d 1188, 1192 (10th Cir. 2009). Authenticom's claims run directly against this body of law, and will inevitably require the Court to engage in the untenable exercise of determining what the proper terms of dealing between Reynolds and Authenticom should be. *Trinko* forbids such a result. *Trinko,* 540 US at 408 ("Enforced sharing also requires antitrust courts to act as central planners, identifying the proper price, quantity, and other terms of dealing-a role for which they are ill suited. Moreover, compelling negotiation between competitors may facilitate the supreme evil of antitrust: collusion.").

Trinko is fatal to Authenticom's Section 2 claims. It is relevant to the Section 1 analysis as well: just as Reynolds has no duty to deal with Authenticom directly, Reynolds also has the unilateral right to control who has access to its system in dealership and vendor customer contracts. *See, e.g., CBC Companies, Inc.*, 561 F.3d at 572-73; CA7 Oral Arg. at 30:05-15 ("That's a kind of vertical agreement and it won't distinguish this case from *Trinko*.") (Easterbrook, J.).[6] And as set forth below, Reynolds's refusal to allow CDK to access the Reynolds DMS necessarily dictated the 2015 wind down agreement (or something just like it) as well. Properly viewed through this lens, Authenticom's theories fall apart as implausible. The self-evident cause of Authenticom's alleged harm is Reynolds's alleged blocking, which is

[6] *See also* CA7 Oral Arg. at 31:30-50 ("Reynolds said, in the world before this agreement, the only way to get access to our system is with our consent and using our portal. It is not sufficient to have the dealer's consent because the dealers are not us. Our consent is required. Now that is a unilateral declaration and it really doesn't make any difference—I don't want you to say, well *Trinko* is distinguishable because that was unilateral and this isn't. Because in *Trinko*, Verizon was dealing with some firms and not dealing with others. It was exercising choice. And that's what Reynolds was doing.") (Easterbrook, J.).

fundamentally a function of neutral system security measures, not contract. Reynolds has the plain right to impose such measures, which means that Authenticom's claims fail.

IV. REYNOLDS IS PRIVILEGED TO UNILATERALLY BLOCK AUTHENTICOM (AND OTHER HOSTILE ACCESS): AUTHENTICOM'S TORTIOUS INTERFERENCE CLAIMS CANNOT STAND

As described above, Reynolds has no duty to provide access to its system to Authenticom. And Authenticom's desired access is illegal. As described in Reynolds's Memorandum, (at 8-9, 47-48), Reynolds had every right to enforce its longstanding policy against unauthorized access. No tortious interference claim can lie.

V. AUTHENTICOM'S JIGSAW OF HORIZONTAL THEORIES CANNOT BE ALLOWED TO PROCEED

In its original complaint, Authenticom alleged that the allegedly illegal horizontal conspiracy was contained within Defendants' written "Wind Down Agreement" from February 2015. Over the course of its Opposition, unable to find a conspiracy in the language of the agreement or support in its complaint, Authenticom now asserts numerous, shifting versions of the alleged conspiracy. Unwound from the puzzle pleading, these theories each fail.

A. At minimum, the Court should rule that the written 2015 agreements do not constitute an illegal horizontal conspiracy

As with Authenticom, Reynolds had the right to exclude CDK's subsidiaries, DMI and IntegraLink, from engaging in hostile access to the Reynolds DMS—both under *Trinko* and under the CFAA. The complaint openly admits that Reynolds made the decision to prohibit such access at least prior to 2010. Compl. ¶¶ 6, 92. As a consequence of that decision (and the technological measures that enforced it), CDK had only two options: wind down its Reynolds-access business in an orderly fashion, or shut it down in a disorderly fashion.

The antitrust laws do not privilege an abrupt wind down over an orderly one. Authenticom attempts to paint the orderliness of the wind down as being "collusive," but the

reality is that CDK had no choice but to end its subsidiaries' hostile integration business—otherwise it faced continued disruption of its customers' access to Reynolds's DMS and potential litigation by Reynolds to forcibly end that access. The only purported "market" being divided was based on accessing Reynolds's DMS,[7] which CDK had no legal ability to do. Reynolds and CDK's agreement to implement an orderly wind down thus was not an illegal restraint of trade. The decision about whether CDK had to "exit" the Reynolds DMS was, per the complaint's own allegations, made unilaterally by Reynolds long prior to 2015. Compl. ¶¶ 6, 92, 189. Authenticom offers no response or rebuttal to this argument, aside from its (incorrect) contention that hostile integration does not run afoul of CFAA. The core of Authenticom's supposed conspiracy is thus not a conspiracy at all.

Authenticom's contentions with respect to the other two 2015 agreements are even weaker. On their face, these agreements are not horizontal agreements between competitors; they are vertical agreements between customer and supplier. The fact that Reynolds and CDK agreed to make their applications available to the other's DMS customers is also indisputably pro-competitive—just as it is for Apple to make iTunes available on Windows and Microsoft to make Office available on iOS. The antitrust laws promote such arrangements, not discourage them.

Accordingly, the Court should hold that the three 2015 agreements, by their plain and unambiguous terms, are not illegal restraints of trade and are entirely legal under Section 1 of the Sherman Act.

B. Authenticom's other conspiracy theories are too vague and implausible to survive *Twombly*

[7] This is reinforced by Authenticom's express allegation that "Reynolds does not compete in the Dealer Data Integration Market outside of the Reynolds DMS." Compl. ¶ 102 n.24.

The bulk of Authenticom's attention is now focused on a mix of alleged conspiracy theories that fall outside of the written 2015 agreements, the primary identified contour of which is that Defendants agreed to "destroy" or "eliminate" Authenticom. Opp. at 12-13. The actual details and mechanics of this supposed conspiracy are essentially left to the imagination, or at best to speculation. Superficially, that works to Authenticom's advantage: it is hard to attack (or evaluate) the plausibility or rationality of a conspiracy sketched with such faint detail. But *Twombly* requires more for that very reason. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-59 (2007).

Moreover, even as articulated, this supposed conspiracy is implausible and even contradicted by several of Authenticom's own pleaded facts. Authenticom alleges in several places in its complaint that Reynolds continues to use Authenticom to pull or cleanse data in certain scenarios for Reynolds's applications. Indeed, Authenticom explicitly alleges that "Reynolds is actually one of Authenticom's larger vendor clients." Compl. ¶ 207. If those allegations are taken as true, a conspiracy to destroy Authenticom would make no sense. Similarly, Authenticom alleges that Reynolds has granted exceptions that allowed Authenticom to access Reynolds's DMS. *Id.* ¶ 205. Taken as true, that allegation is irreconcilable with the notion that Reynolds is boycotting Authenticom—much less that it agreed to do so with CDK. There is no plausible conspiracy here where there is no possibility that CDK could actually enforce it against Reynolds and Authenticom affirmatively pleads that any such conspiracy *was not enforced*. *See Matsushita Elec. Indus. Co., Ltd. v Zenith Radio Corp.*, 475 US 574, 588 (1986) (evaluating an ambiguously plead Section 1 conspiracy requires the Court to "consider the nature of the alleged conspiracy and the practical obstacles to its implementation"). Instead, the only plausible conclusion from such facts is that each defendant was individually

determining whether, when, and how to do business with Authenticom as they each saw fit. That destroys any notion of conspiracy.

Authenticom attempts to offer one "rational motive" explanation in its brief when it contends that CDK rationally wanted Reynolds's assurance that it would maintain its longstanding computer system design and policies prior to CDK deciding to embark on a similar course. Opp. at 22-23. This new conspiracy theory appears nowhere in the complaint. It also concerns a conspiracy regarding neutral DMS design decisions that is very distinct from the supposed conspiracy to "destroy" Authenticom. This type of sleight of hand runs throughout Authenticom's conspiracy arguments, which is precisely why it wants to avoid pinning down its actual conspiracy allegations with any coherent detail. Moreover, even this supposedly "rational" explanation is still entirely implausible. Authenticom's own allegations plainly establish that Reynolds's commitment to an access-restricted DMS design had been unwavering since at least 2006 and was well known throughout the industry. Compl. ¶¶ 6, 92. The notion that CDK needed some assurance that Reynolds would continue doing what it had always done falls far short of the type of reasonable inference that is permissible (and required) to support an antitrust claim. *See Matsushita*, 475 U.S. at 588 (holding that an antitrust plaintiff "must show that the inference of conspiracy is reasonable in light of the competing inferences of independent action or collusive action that could not have harmed [the plaintiff]"). Though Authenticom did not feel constrained by its pleading in response to the motion to dismiss, it was unable to point to a single piece of evidence (hearsay or otherwise) that would indicate anyone in the industry—least of all CDK—had any concern that Reynolds would soon reconfigure and "open" its system to Authenticom or any other hostile integrator. CDK did not need, want, or get any assurance from Reynolds—and Authenticom has no evidence that it did.

Authenticom's reliance on *In re High Fructose Corn Syrup* is also entirely inapt. *See In re High Fructose Corn Syrup Antitrust Litig.*, 295 F.3d 651, 654–55 (7th Cir. 2002). The Seventh Circuit's remark regarding an admitted price fixing conspiracy is a red herring, as Authenticom has neither alleged price fixing nor described the actual terms or mechanics of the supposed conspiracy—much less provided "admissions" of them. The Seventh Circuit highlighted in that case that there must be "an express, manifested agreement" to satisfy Section 1. *Id.* at 654. The only manifested agreements that Authenticom has identified are the February 2015 agreements—legitimate vertical agreements winding down unauthorized access and providing for additional cross-platform application market competition.

C. There is no causal nexus between the alleged conspiracy and Authenticom's alleged harm

Underscoring all of these issues, Authenticom continues to face the problem that its supposed injuries all flow from the denial of access to Defendants' proprietary systems and software. As set forth above, given Reynolds's unilateral decision to deny access to hostile integrators and malicious computer intruders alike, Authenticom has no right to such access under *Trinko*. As further explained above, Authenticom's efforts to obtain such access without permission are illegal under the CFAA, which deprives Authenticom of any valid antitrust injury. But the complaint also underscores that the true origin of Authenticom's alleged harm, especially as to Reynolds, is the technological security measures that keep Authenticom off the DMS. As the complaint highlights, Reynolds's unilaterally-designed closed system and robust security protocols—not any antitrust violation—effectively eliminated Authenticom's hostile access to the Reynolds DMS in 2013, two years before any alleged horizontal agreement. Compl. ¶ 189. Without a viable antitrust injury or causal nexus to its alleged harm, an antitrust plaintiff may not proceed. *See, e.g.*, *O.K. Sand & Gravel v. Martin Marietta Techs.*, 36 F.3d

565, 573 (7th Cir. 1994) ("To establish an antitrust injury, a plaintiff must show not only that the injury is of the type intended to be protected by the antitrust laws, but that the violation was 'the cause-in-fact of the injury: that 'but for' the violation, the injury would not have occurred.'" (quoting *Greater Rockford Energy & Tech. Corp. v. Shell Oil Co.*, 998 F.2d 391, 394–96 (7th Cir. 1993))).

D. At bottom, Authenticom relies on alleged price increases that went into effect *well before any conspiracy*

Unable to demonstrate any actual conspiracy, Authenticom claims that the effects of such a conspiracy can be seen in price increases charged to vendors for DMS integration. *See* Compl. ¶ 176; Opp. at 3. But (presumably) the alleged conspiracy was on or around the time of the February 2015 agreements. While reaching well beyond its complaint to find evidence that might allow its conspiracy allegations to survive, Authenticom artfully ignores the evidence it adduced of the *timing* of Reynolds's alleged price increases: all of the underlined increases *were well before any alleged conspiracy*. *Compare* Opp. at 16 (complaining of allegedly sharp price increases but not noting the *date* of those increases) *with* the cited testimony at Dkt. 165 at 54:3-9 (making clear that those alleged increases were *in* ***2013*** and earlier, years before any alleged conspiracy).

While Reynolds does not dispute that its technology and contracts "block" Authenticom (and malicious hackers alike), there is no dispute that Reynolds does so based on decisions made unilaterally years before any alleged conspiracy. Authenticom's claims based on an implausible conspiracy must be dismissed.

VI. AUTHENTICOM'S OTHER ANTITRUST THEORIES ALSO FAIL

A. Authenticom's tying claim fails as a matter of law

Authenticom claims that Reynolds's longstanding unilateral prohibition on unauthorized third-party access constitutes an illegal "tying" arrangement with its dealers. According to Authenticom, the "tying" product is the DMS itself and the "tied" product is Reynolds's (single-brand) "integration services." Dkt. No. 216 at 35. Assuming *arguendo* that Reynolds's DMS and "integration services" are two distinct products—which Reynolds disputes—Authenticom's tying claim still fails to survive a motion to dismiss for at least three reasons.

1. Reynolds has the unilateral right to exclude Authenticom

First, Authenticom's "tying" claim is just an attempt to end-run *Trinko*—to which Authenticom has no answer. Reynolds has the unilateral right to grant or deny access to its system, and has no duty to facilitate, "protect", "whitelist", or otherwise help Authenticom peddle its [illegal] trade. *See Trinko*, 540 U.S. at 408; *Linkline*, 555 U.S. at 448. Reynolds's contracts with its DMS customers are alleged to constitute tying because they prohibit dealers from granting system access to unauthorized third parties. As described above, under *Trinko*, Reynolds has the legal right to prohibit such access to its system, courts have been cautioned not to oversee forced dealing, and Authenticom's desired trade is, in any event, illegal.

2. Authenticom fails to allege that Reynolds has market power in the tying product

Second, it has long been the rule in the Seventh Circuit that "a tying agreement is not actionable unless the defendant has substantial market power in the tying product." *Hardy v. City Optical Inc*. 39 F.3d 765, 767 (7th Cir. 1994) (emphasis added). The Supreme Court has also "moved from relying on assumptions to requiring a showing of market power in the tying product," as the Court's disapproval of tying arrangements "has substantially diminished." *Illinois Tool Works Inc. v. Independent Ink, Inc.*, 547 U.S. 28, 35 (2006).

In its response, Authenticom appears to recognize that it must plead that Reynolds has market power in the DMS market, but Authenticom cannot point to anywhere in its complaint that it has done so.

Authenticom's response cites to 13 paragraphs in the complaint for the purported proposition that "Defendants have successfully imposed significant price increases for DMS software—untethered to costs—without losing many dealers to rivals." Opp. at 37 (citing Compl. ¶¶ 214-225, 257). However, virtually all of the cited paragraphs contain allegations of pricing for *integration*—the ostensibly "tied" product—not DMS pricing. The only fact alleged regarding Reynolds's DMS pricing is that the "standard Reynolds contract provides that DMS fees go up every year on March 1 . . . and is measured by the Customer Price Index plus 2%." Compl. ¶ 225. This unremarkable allegation comes nowhere close to demonstrating "substantial DMS market power" by Reynolds.

Moreover, despite the assertion in Authenticom's response that Reynolds has raised prices "without losing many dealers to rivals," Authenticom's complaint does not actually include any such allegation. Simply put, Authenticom does not and cannot allege that Reynolds has market power in the DMS market.

Authenticom's suggestion that Reynolds's alleged 30% market share "confirms" Reynolds's market power misses the mark for at least two reasons. First, if Authenticom wishes to rely on the injunction record, then Authenticom cannot have it both ways: the Court has already noted (in reliance on Authenticom's own expert's testimony) that Reynolds's market share has declined to 28 percent. Dkt. 172 at 6 (citing Dkt. 165 at 84:7-17). Second, in any event, Authenticom's interpretation of *Hardy* to mean that a market share of 30% or higher is sufficient to establish market power is misplaced. In fact, the Seventh Circuit case upon which

Hardy relies makes clear that in *Jefferson Parish*, the Supreme Court assumed a market share of 30% and still concluded that to be **in**sufficient. *Will v. Comprehensive Accounting Corp*., 776 F.2d 665, 672 (7th Cir. 1985) (citing *Jefferson Par. Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 26-28 & n.43 (1984)). *Will* goes onto note that DOJ guidelines "accurately reflect this authority in treating as lawful any tying arrangement affecting less than 30% of a relevant market." *Id*. These authorities, if anything, conclusively establish that Reynolds *lacks* market power in the DMS market.

3. There is no tying because different buyers purchase the alleged tying product (DMS) and tied product (integration interfaces)

Even putting aside Authenticom's failure to plead market power on the part of Reynolds, the tying claim fails to survive a motion to dismiss because it does not meet the basic definition of the doctrine. Both the Supreme Court and the Seventh Circuit have defined tying as "an agreement by a party to sell one product but only on the condition that ***the buyer*** also purchases a different (or tied) product, or at least agrees that he will not purchase that product from any other supplier." *Reifert v. South Cent. Wis. MLS Corp*., 450 F.3d 312, 322 (7th Cir. 2006) (Wood, J., concurring) (citing *Northern Pacific Ry. Co. v. United States*, 356 U.S. 1, 5-6 (1958)) (emphasis added). As set forth in Reynolds's Memorandum (at 42-43), this is fatal to Authenticom's claim, because it is acknowledged on the face of the complaint that while auto dealers license DMS platforms, application vendors (a different "buyer" altogether) license integration interfaces. *See* Dkt. 176 at 42-43.

In response, Authenticom cites no case allowing a tying claim to go forward when the buyers of the "tying product" and the "tied product" are different. Instead, it cites two cases that do not involve tying claims at all. See Dkt. 216 at 38 (citing *American Needle, Inc. v. NFL*, 560 U.S. 183, 193 (2010); *Dos Santos v. Columbus-Cuneo-Cabrini Med. Ctr*., 684 F.2d 1346, 1354

(7th Cir. 1982)). But *American Needle* states only the unremarkable proposition that the Sherman Act "is aimed at substance rather than form," but whether substance or form is the test – *vendors license integration.* Vendors determine if they want to support their product with real-time, batch, or some hybrid integration. Vendors negotiate integration licensing contracts. And vendors, not dealers, are the buyers of integration. That is true whether the vendors are customers of Reynolds's real integration; or pay Authenticom for hostilely scraped data—a vendor decision over which *dealers* have no control.

Likewise, the *Dos Santos* opinion includes dicta that for purposes of defining a market for anesthesia services, it "may" be more appropriate to treat hospitals as purchasers, rather than patients, because patients do not make "any significant economic decision." 684 F.2d at 1354. In addition to its cautious phrasing and the fact that it does not involve a tying claim, *Dos Santos* is factually inapposite to the present case. According to Authenticom's own complaint, application vendors make the primary decision on which "data integration services" to purchase. Compl. ¶¶ 14, 60, 148, 187, 232. The argument in Authenticom's response that "dealers still control the selection of integration services and are thus the subjects of the illegal 'forcing'" is not only conclusory, it is unsupported by Authenticom's complaint. For this additional reason, Authenticom's tying theory should be dismissed.

B. Similarly, Authenticom's exclusive dealing allegations fail

Like its tying claims, Authenticom's allegations that Reynolds's prohibitions against unauthorized system access in Reynolds's dealer and vendor licensing agreements are illegal "exclusive dealing" arrangements likewise fail. Again, this is an end-run against Reynolds's unilateral right to deal or not deal with third parties. Just as Reynolds has the right not to deal with Authenticom directly, so too does it have the right not to allow its dealers or vendor customers to assign or sublicense their DMS access privileges to others: "[t]he exclusion of

competitors is cause for antitrust concern only if it impairs the health of the competitive process itself." *Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 394 (7th Cir. 1984) (citing *Prod. Liab. Ins. Agency, Inc. v. Crum & Forster Ins. Cos.*, 682 F.2d 660, 663-65 (7th Cir. 1982)). As a business decision consonant with its long-standing strategy to maintain a secure, reliable, premium DMS, Reynolds legitimately can decide to license direct DMS access to third-party vendors only through RCI. *See Jack Walters & Sons Corp. v. Morton Bldg., Inc.*, 737 F.2d 698, 710 (7th Cir. 1984) ("Vertical integration is a universal feature of economic life and it would be absurd to make it a suspect category under the antitrust laws just because it may hurt suppliers of the service that has been brought within the firm.").

Additionally, this theory cannot be sustained given the terms of Reynolds's actual contracts. *See* Reynolds Interface Agreement (ECF 185-3); Reynolds Master Agreement (ECF 185-1).[8] None of Reynolds's contracts affects vendors' ability to use Authenticom to access any other DMS, including CDK's. Vendors in the RCI program also remain free to use Authenticom for Reynolds's customers when the data is supplied by the dealer. *See* Compl. ¶ 104. The singular restriction in Reynolds's vendor contracts is that they not simultaneously engage or participate in unauthorized access to Reynolds's DMS while using RCI. ECF 185-3, § 2.5.3. That falls far short of "exclusive dealing." And Reynolds's dealer customers, in any event, remain free to switch to open DMS systems that allow data syndication by Authenticom to its vendor customers—a fact that "negate[s] substantially [the agreements'] potential to foreclose competition." *Omega Envtl., Inc. v. Gilbarco, Inc.*, 127 F.3d 1157, 1163-64 (9th Cir. 1997) (citing *Roland Mach.*, 749 F.2d at 394-95) (additional citations omitted); *see also Methodist Health Servs. Corp. v. OSF Healthcare Sys.*, 859 F.3d 408, 410 (7th Cir. 2017).

[8] As set forth in the original Memorandum, consideration of these agreements is appropriate. *See* Memo. at 6.

For this reason, and the additional reasons outlined in Reynolds's Memorandum (at 43-47), Authenticom's exclusive dealing claims must fail.

C. Single-brand aftermarket claims under *Kodak* are strictly limited, and do not survive here, given Reynolds's longstanding contracts and policies admitted in the complaint

A single-brand aftermarket claim[9] – that is, that Reynolds controls the market of its own brand of integration applicable only to dealers who license a Reynolds DMS – is strictly limited. And where dealers enter contracts with full knowledge that they must not use other forms of hostile access—as Authenticom admits Reynolds's DMS customers do—no *Kodak* claim can lie. Period. This claim too, must fail.

Eastman Kodak Co. v. Image Tech. Servs., 504 U.S. 451 (1992), is a narrow and, of late, rarely used exception to the general rule that where there is competition in a primary market (here, the DMS market), antitrust claims based on monopolization of secondary "after markets" will not stand. Authenticom's complaint fails to adequately plead that the *Kodak* exception applies.

According to the Seventh Circuit, the salient facts of Kodak are as follows:

- Kodak sold copiers in a market with three substantial rivals.
- At the time of sale, Kodak sold replacement parts, enabling users to repair their copiers or hire independent service organizations (ISOs) to do so.
- Later Kodak ***changed its policy*** and refused to sell parts to ISOs, who alleged that this enabled Kodak to claim the repair business for itself, at supra-competitive prices.

Digital Equip. Corp. v. Uniq Digital Techs., Inc., 73 F.3d 756, 762 (7th Cir. 1996) (citing *Kodak*).

[9] In a single-brand aftermarket, the brand owner necessarily has "100%" of the market. Authenticom presumably attempts to plead this rarely-found claim because Reynolds does not have market power in the primary, relevant, DMS market.

Virtually all courts agree that the *Kodak* holding rested in part on the fact that Kodak *changed* its policies such that customers could not have known about Kodak's prohibition against third-party parts suppliers when the customers bought Kodak copy machines. As the Seventh Circuit has explained, the result in *Kodak* would have been different if either of the following facts had been true:

- Spare parts had been bundled with Kodak's copiers from the outset; or
- Kodak had informed customers about its policies before they bought its machines.

Digital Equip., 73 F.3d at 763. ("The Court did not doubt in *Kodak* that if spare parts had been bundled with Kodak's copiers from the outset, or Kodak had informed customers about its policies before they bought its machines, purchasers could have shopped around for competitive life-cycle prices.")

Applying those concepts to Authenticom's claims here, Authenticom pleads itself out of a claim. According to Authenticom's complaint, Reynolds's standard DMS contract unequivocally "prohibits dealers from providing access to the DMS to any third party." Compl. ¶ 152. Likewise, Authenticom alleges that the "Reynolds DMS Customer guide, which is incorporated into the contract, similarly states that the dealer is barred from 'permitting any person, firm or entity access to' the DMS." *Id*. Authenticom has not alleged that these contracts changed at any time.

Moreover, Reynolds's prohibition on third-party access was not disclosed solely in the contracts. According to Authenticom's complaint, Reynolds "closed system" policies have been widely discussed in the industry press for over a decade. *See* Compl. ¶¶ 6, 65 n.6, 70 nn.10-11, 74 n.13) (citing news articles from 2006-2011).

The fact that Reynolds's contracts admittedly prohibited system access by third parties like Authenticom and such prohibitions were widely reported and known in the industry ends the *Kodak* inquiry. Full stop. *Kodak* is a limited and rare exception that has no place in this litigation.

Authenticom makes three basic arguments in its Opposition. First, Authenticom argues that CDK's contracts allow dealers to authorize "agents." Dkt. 216 at 43. Whatever significance this argument has (if any), Authenticom does not and cannot assert it with respect to Reynolds's contracts. Authenticom does not allege that anything in Reynolds's contracts are even ambiguous on third-party access—let alone that they allow it.

Second, Authenticom argues that the "actual real-world policies with regard to third-party integration services changed after the dealers were already locked-in." *Id*. This argument too focuses mostly on CDK, but Authenticom goes on to contend that Reynolds "changed its policy *with regard to enforcement*" of its DMS agreements, given that its technical blocking become "more aggressive" from 2009-2013. *Id*. at 43-44. Not surprisingly, Authenticom points to no case suggesting that a plaintiff can claim ignorance of a prohibition unambiguously stated in a written contract (much less one that was widely publicized in the press) merely because the affirmative "enforcement" of that prohibition became "more aggressive" (or effective) over time.

Finally, Authenticom argues that it is ultimately a factual question whether a customer would understand the contract, relying primarily on *Datel Holdings Ltd. v. Microsoft Corp*., 712 F.Supp.2d 974 (N.D. Cal. 2010). In *Datel*, however, the relevant contract language was hotly disputed, and the court determined that the plaintiff had "at the very least . . . shown an ambiguity in the relevant contract language which counsels against granting a motion to dismiss premised on Defendant's contested interpretation of the provision, which [individual video game

console purchaser] customers may not have understood." *Id*. at 989. Here, Authenticom has not pleaded—let alone established—any ambiguity in the contract. Indeed, it affirmatively alleges that the policy at issue was publicized for the masses in the industry press.

At the end of the day, Authenticom's pleadings acknowledge that Reynolds has barred third-party access to its DMS for at least a decade. This alone dooms Authenticom's attempt to cram the allegations against Reynolds into a *Kodak* claim.[10]

VII. CONCLUSION

For these reasons and those set forth in the Memorandum, Authenticom's claims should be dismissed with prejudice.

[10] While the Court need not reach the issue of "lock in" or "switching costs," it is worth noting that Authenticom's complaint acknowledges that switching DMS providers is entirely possible (*see* Compl. ¶ 102); and this Court has previously noted the marked effects of that switching on market shares. *See* Dkt. 172 at 6. Authenticom's reference to its allegation that the "average DMS tenure is more than 20 years" is beside the point. Authenticom acknowledges that the average length of each contract is only 5 years, and does not allege that a single current contract was signed at a time when Reynolds's third-party access policies were unclear.

DATED: October 6, 2017

Respectfully submitted,

/s/ *Aundrea K. Gulley*

John S. Skilton
JSkilton@perkinscoie.com
Charles G. Curtis, Jr.
CCurtis@perkinscoie.com
Michelle M. Umberger
MUmberger@perkinscoie.com
Brandon M. Lewis
BLewis@perkinscoie.com
Jesse J. Bair
JBair@perkinscoie.com
PERKINS COIE LLP
One East Main Street, Suite 201
Madison, WI 53703
Telephone: 608-663-7460
Facsimile: 608-663-7499

Kathleen A. Stetsko
KStetsko@perkinscoie.com
PERKINS COIE LLP
131 South Dearborn St., Suite 1700
Chicago, IL 60603
Telephone: 312-324-8400
Facsimile: 312-324-9400

Kathy Patrick
kpatrick@gibbsbruns.com
Aundrea K. Gulley
agulley@gibbsbruns.com
Brian T. Ross
bross@gibbsbruns.com
Brice A. Wilkinson
bwilkinson@gibbsbruns.com
Ross M. MacDonald
rmacdonald@gibbsbruns.com
GIBBS & BRUNS, LLP
1100 Louisiana, Suite 5300
Houston, Texas 77002
Telephone: 713-650-8805
Facsimile: 713-750-0903

Michael P.A. Cohen
MCohen@sheppardmullin.com
Amar S. Naik
ANaik@sheppardmullin.com
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Suite 100
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Telephone: 202-747-1900
Facsimile: 202-747-1901

Attorneys for Defendant
The Reynolds and Reynolds Company